2018年6月25日
株式会社みずほフィナンシャルグループ

「サイバーセキュリティ経営宣言」の策定について

株式会社みずほフィナンシャルグループ（執行役社長：坂井 辰史）およびグループ各社（※1）は、日本経済団体連合会（以下「経団連」）が2018年3月に公表した「経団連サイバーセキュリティ経営宣言」を受け、このたび、「サイバーセキュリティ経営宣言」を策定しました。

経団連はSociety 5.0の実現に向け、情報共有や人材育成等官民が取り組むべきサイバーセキュリティ対策についてさまざまな提言を行っています。そのような中、「経団連サイバーセキュリティ経営宣言」は、サイバーセキュリティ対策の意義を広く共有し、経済界が一丸となって取り組みを加速させていく重要性について説明しています。

経団連の取り組みを受け、〈みずほ〉は、サイバーセキュリティ対策の重要性を認識し、サイバー攻撃を経営上のトップリスクの1つと位置づけ、戦略を策定しています。また、Mizuho-CIRT（※2）を中心に、高度なプロフェッショナル人材を配置し、外部の専門機関とも連携したインテリジェンスや先進技術も駆使しながら、統合SOC（※3）等による監視や、ウィルス解析、多層的防御等レジリエンス態勢(※4)強化に取り組むとともに、中長期的な視点での人材育成にも注力しています。

〈みずほ〉は、本宣言を通じ、金融という重要な社会インフラの担い手として、主体的にサイバーセキュリティ対策を推進するとともに、安心・安全なサイバー空間の構築に貢献していきます。

以　上

（※1）みずほ銀行、みずほ信託銀行、みずほ証券、アセットマネジメントOne、
みずほ総合研究所、みずほ情報総研、みずほプライベートウェルスマネジメント、
資産管理サービス信託銀行
（※2）Cyber Incident Response Teamの略
（※3）Security Operation Centerの略
（※4）サイバー攻撃によって生じる被害を最小限に抑え、素早く復旧し、業務を
継続できるようにすること

「サイバーセキュリティ経営宣言」

1. 経営課題としての認識
   - ■ 経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組みます。
   - ■ 経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組みます。

   お客さまに安心して金融サービスをご利用いただくとともに、金融インフラの安定稼動と持続的発展に貢献するため、サイバー攻撃を経営上のトップリスクの１つと位置づけ、経営主導のもと、定期的に議論したうえで、経営資源を適切に配分し、態勢強化に取り組みます。

2. 経営方針の策定と意思表明
   - ■ 特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP(事業継続計画)の策定を行います。
   - ■ 経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努めます。

   年次で見直すサイバーセキュリティ戦略に基づいて、Mizuho-CIRTを中心に、統合SOC等による監視、ウイルス解析、多層的防御等、レジリエンス態勢の強化に着実に取り組みます。
   また、統合報告書や当社ホームページ等を通じて、サイバーセキュリティ態勢強化の取り組みの開示に努めます。

3. 社内外体制の構築・対策の実施
   - ■ 予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じます。
   - ■ 経営・企画管理・技術者・従業員の各層における人材育成や教育を行います。
   - ■ 取引先や委託先、海外も含めたサプライチェーン対策に努めます。

   サイバーセキュリティに精通した高度なプロフェッショナル人材の育成を、中長期的に取り組むべき重要な課題と認識し、外部の専門機関とも連携しながら、人材発掘と動機付けに取り組みます。
   また、経営も参加した訓練や、業界横断での演習への参加を通じて、社内体制や対策の実効性を向上します。
   委託先等でのセキュリティ対策状況のモニタリング等を通じ、サプライチェーン対策に努めます。

4. 対策を講じた製品・システムやサービスの社会への普及

■ 製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努めます。

犯罪被害からお客さまの資産を守るため、インターネットバンキングなどのサービスにおいて、お客さまの端末へのウイルス駆除ソフトの導入や認証の高度化、取引のモニタリングなど、さまざまなセキュリティ対策を実施します。
また、ホームページ等を通じ、パスワード悪用やウイルス感染への注意等、安全にご利用いただくための対応を呼びかけます。

5. 安心・安全なエコシステムの構築への貢献

■ 関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図ります。

■ 各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与します。

この「つながる社会」の時代、サイバーセキュリティを守るもの同士が、平時・有事とも、さらに高度に連携していく必要があると考え、政府機関や監督当局、警察などの法執行機関や金融 ISAC、FS-ISAC と、「信頼しあえる、双方向のコミュニケーション関係」を構築できるよう、働きかけます。
また、調査や解析活動によって得られた情報を、積極的に外部に提供することにより、社会全体のサイバーセキュリティ強化に努めます。